Несмотря на определяющую роль самостоятельной работы в обучении с применением компьютерных технологий, основными субъектами учебного процесса являются студент и преподаватель. Соучастие студента в познавательной деятельности наравне с преподавателем есть одно из условий качественного образования, как в традиционной системе, так и в ДО. Поэтому основным требованием к технологиям дистанционного обучения является сохранение преимуществ очного обучения на расстоянии. Использование сформулированных выше принципов при разработке учебно-методического обеспечения позволяет в максимальной степени удовлетворить этим требованиям.

Самченко В.А., ЕЭТК МТО
гр. П-73
Руководитель: преподаватель высшей категории
Н.В. Порошина

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ВИРУСНЫХ АТАК

В нашей жизни различного рода информация играет очень важную роль. И в большинстве своем она в нужном нам виде храниться на компьютере. На домашнем компьютере редко кто работает с документами, таблицами, базами данных и прочими сложными видами хранения информации. В большинстве случаев всем этим мы занимаемся на работе. Но мало кто догадывается, какой опасности иногда подвергается все месячные/годовые отчеты по бухгалтерии, счет-сметы и тому подобные виды очень важной для стабильной работы информации в виде различного рода документов, бережно раскладываемых по разным папкам и дискам в рабочем компьютере. Вся наша бережно хранимая почта с логинами и паролями от различного рода интернет-сервисов. Фотографии родных, с таким трудом найденные и бережно хранимые песни нашей юности. Программы, позволяющие нам с легкостью и быстротой выполнить ту или иную задачу. И ведь все это может быть утеряно в один единственный миг, утеряно без возможности восстановления.

Мы не будем сейчас рассматривать все возможные причины такого исхода событий. Не будем сваливать все на полумифических, и от этого еще более неизвестных и пугающих хакеров. Также не будем рассматривать ошибки аппаратные, как то: внезапное отключение питания или конфликты в оборудовании.

Мы возьмем лишь две проблемы безопасности данных – это несанкционированный доступ и атака компьютерным вирусом.

Возьмем в качестве исследуемого «стенда» компьютерный класс, состоящий из десяти рабочих компьютеров и одного администраторского. Все они объединены в одну локальную сеть, подключение к интернету отсутствует. Согласно определению, данному в учебнике информатики для старших классов: «ИС является средой, составляющими элементами которой являются компьютеры, компьютерные сети, программные продукты, базы данных, люди, различного рода технические и программные средства связи и т.д. Основная цель информационной системы – организация хранения и передачи информации» наш «стенд» является *информационной системой.*

Так какие же меры нужно предпринимать, чтобы оградить себя и подведомственную вам информационную систему от возможных проблем? Так как мы для рассмотрения взяли две причины – Несанкционированный доступ и Компьютерные вирусы, то рассмотрим их каждый по отдельности:

Начнем с самого простого: *Вирусная опасность.*

Видов компьютерных вирусов существует превеликое множество, их список вправе может соперничать со списком человеческих болезнетворных вирусов, но нас интересует лишь один их вид, самый опасный: «троянские» программы (Trojan). Такой вид компьютерных вирусов может запросто «положить» систему в считанные минуты, все зависит от специфики и назначении вируса. Так откуда же могут взяться вирусы на компьютерах, не подключенных к интернету? Все очень просто: люди, работающие за этими компьютерами, могут принести их на рабочие места посредством флэшек, сд-дисков, дискет, портативных HDD и т.п. В таком случае с зараженного носителя информации «злобный зверек» быстро «десантируется» на благодатную для его действий почву. Последствия могут быть очень печальными, а могут просто сказаться на скорости работы компьютеров. Напоминаю – все зависит от специфики и назначения вируса.

Решение – установка на каждый компьютер хорошей антивирусной программы с установкой сервера обновления сигнатур вирусов на административном компьютере. В нашем случает на «стенде» на каждый из рабочих компьютеров был установлен антивирус ESET NOD32 Antivirus, на административный – ESET NOD32 Antivirus Business Edition с настройкой зеркала обновления. За время работы не было замечено ни одной вирусной опасности, влияющей на работу ИС. Все проявления вирусной активности были вовремя замечены и предотвращены.

Перейдем к проблеме куда более реальной и сложной: *Несанкционированный доступ к компьютерной информации.* Под несанкционированным доступом понимают действие, направленное на получение информации и привилегий лица, не обладающего необходимым разрешением и полномочиями для выполнения данных действий законным и установленным путем. Обычно действиям такого плана предшествует взлом или обход систем безопасности, если таковые присутствуют. К примеру на нашем «стенде»: какое-то либо лицо, имеющее своей целью завладеть (к примеру) важными документами, хранящимися на одном из рабочих компьютеров, пробирается на рабочее место в отсутствие сотрудника и копирует нужную ему информацию без права доступа к ней.

Результат: утечка важной информации (к примеру) в конкурирующую фирму.

Как такое предотвратить? Во-первых, нужно четко регламентировать права доступа к рабочим местам. Во-вторых, установить на учетную запись, под которой работает сотрудник, сложный многозначный пароль, установить права доступа в личную шифрованную папку данного сотрудника, установить систему учета и регистрации индикации входа в учетную запись каждого рабочего места на административном компьютере. В-третьих, защитить другой возможный доступ, не связанный с использованием учетной записи данного работника: т.е. защитить шифрованием весь жесткий диск и каждый раздел в нем присутствующий, предотвратить использование (а также создание) других (посторонних) учетных записей, не учтенных регламентационным порядком. В-четвертых, исключить все возможные методы обхода и устранения защиты. И в-пятых, запретить нахождение и пропуск посторонних лиц, не учтенных в регламентированном порядке, ни в рабочее, ни в не рабочее время.

Все указанные шаги и способы были проведены на тестовом «стенде». Проблем утечки информации не обнаружено.

Итак, подведем итог. Информация в любом виде для нас играет очень важную роль. Будь то компьютеризированный вариант, или какой другой. И на первом месте всегда стоит безопасность этой информации.